COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE

500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

June 14, 2007

To: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
Chief Information Officer

Subject: **FISCAL YEAR 2007-08 BUSINESS AUTOMATION PLAN SECURITY SURVEY**

Attached is an assessment of the Fiscal Year 2007-08 Business Automaton Plan (BAP) Security Survey that is completed annually by each department. The information compiled was based on departmental responses to survey questions and used to develop a security effectiveness rating for each department. While many factors were assessed, the last row in the attached matrix reflects the overall assessment by department of compliance with Board adopted security policies and standards.

The majority of departments were rated with some deficiencies (yellow) while 11 departments were rated good (green). Five departments were noted with major deficiencies (red) for various reasons such as security updates not being current or failure to require Acceptable Use Agreements (Board Policy 6.101) to be signed as a condition to use County systems. Departments that have obsolete operating systems were noted as deficient because those systems cannot be updated with current security software that would protect them from viruses. The inability to maintain current security software levels can lead to enterprise-wide security events affecting the County's ability to provide public services.

Since the Security Survey is part of the annual BAP process and is a self assessment of compliance, my Office has engaged the Institute for Critical Information Infrastructure Protection that is part of the University of Southern California, Marshall School of Business to conduct four independent security reviews per quarter of selected County departments. The purpose of the reviews is to independently validate the responses provided in the annual Security Survey. The results of the reviews will validate compliance and identify areas requiring improvement to assist departments in strengthening their information security programs.

Security Reviews are scheduled to begin in July 2007 and will continue over the course of the calendar year. All findings will be provided to the affected departments as well as the Chief Executive Officer, Auditor-Controller, and your Board. Departments will be expected to develop corrective action plans to remediate all areas of weakness noted.

If you have any questions, please contact me or Al Brusewitz, Associate CIO, at (562) 940-3873 or e-mail to abrusewitz@cio.lacounty.gov.

JWF:AB:ygd

Attachment

c: Department Heads
Department CIOs

P:\Final Documents\CIO\CIO Memo-2007 Security Survey 6-7-07 (2) (2) (3).doc

Information Security Survey 2007

Question	Affrm Act	AWM	APD	Anm Cntl	Assessor	A/C	DBH	BOS
Compliant with Board security policies	No	No	Yes	No	Yes	Yes	No	Yes
If not,do you have a compliance plan	Yes	Yes	N/A	No	N/A	N/A	Yes	N/A
Will you be compliant in 2007/2008	Yes	Yes	N/A	No	N/A	N/A	Yes	N/A
Designated security officer	Full time	Part time	Full time	Full time	Part time	Part time	Part time	Part Time
Attend ISSC regularly	No	Yes	Yes	No	Yes	Yes	No	Yes
CCERT participation	Yes	Yes	Yes	No	Yes	Yes	No	Yes
SET participation	No	Yes	Yes	No	Yes	Yes	No	Yes
Have a department computer emergency resp. (DCERT)	No	Yes	Yes	No	Yes	Yes	No	Yes
Systems implemented and configured to security standards	Yes	No	Yes	No	Yes	No	No	Yes
Employees sign acceptable use agreement	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Passwords changed every 90 days	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Physical security measures in place	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Formal security development lifecycle	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vulnerability assessment scanning performed	No	No	Yes	No	Yes	No	No	Yes
Remote access to servers allowed	No	No	No	No	No	Yes	No	Yes
Two Factor authentication required for remote access	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Have identified specific remote access software	No	No	N/A	No	No	No	No	No
Require remote access via VPN	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do you have obsolete computer operating systems	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do you have a technology refresh plan	No	No	No	Yes	No	Yes	No	No
Do you rerquire firewalls on desktops and laptops	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Host intrusion on servers	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Is antivirus software installed and current	No	No	No	No	Yes	Yes	Yes	Yes
Is antivirus software centrally managed	Yes	Yes	Yes	No	Yes	Yes	No	No
Is patch management software utilized	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Are security software patches current	Yes	No	Yes	No	Yes	Yes	Yes	Yes
BCP Plan	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Crisis Mgmt Plan	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes

Departmental Security Rating	□	▓	░	▓	░	□	□	░

Color Codes

Good Security Program	░
Some Deficiencies	□
Major Weaknesses	▓
Not Applicable	N/A

Information Security Survey 2007

Question	CAO	CIO	CSSD	DCFS	Com Dev	CSS	Consumer	Coroner
Compliant with Board security policies	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	Yes	N/A	N/A	N/A	N/A
Will you be compliant in 2007/2008	N/A	N/A	N/A	Yes	N/A	N/A	N/A	N/A
Designated security officer	Part Time	Full Time	Part Time	Part Time	Part Time	Part Time	Part Time	Part Time
Attend ISSC regularly	No	Yes	Yes	Yes	Yes	Yes	No	No
CCERT participation	No	Yes	Yes	Yes	Yes	Yes	No	No
SET participation	No	Yes	Yes	Yes	Yes	Yes	No	No
Have a department computer emergency resp. (DCERT)	No	Yes	Yes	Yes	No	Yes	No	No
Systems implemented and configured to security standards	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Employees sign acceptable use agreement	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Passwords changed every 90 days	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Physical security measures in place	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Formal security development lifecycle	No	Yes	Yes	No	No	Yes	Yes	No
Vulnerability assessment scanning performed	No	No	No	No	Yes	No	No	No
Remote access to servers allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	No	No	No	No	Yes	No	No	No
Have identified specific remote access software	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Require remote access via VPN	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Do you have obsolete computer operating systems	No	No	No	Yes	No	No	No	No
Do you have a technology refresh plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you rerquire firewalls on desktops and laptops	Yes	N/A	Yes	No	No	No	No	No
Host intrusion on servers	No	Yes	No	No	No	No	Yes	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crisis Mgmt Plan	Yes	Yes	Yes	Yes	No	No	No	No

Departmental Security Rating		░	░	█				

<u>Color Codes</u>

Good Security Program	░
Some Deficiencies	
Major Weaknesses	█
Not Applicable	N/A

Information Security Survey 2007

Question	Counsel	DA	Fire	DHS	Hum Rel	DHR	ISAB	ISD
Compliant with Board security policies	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Will you be compliant in 2007/2008	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Designated security officer	Part Time	Part Time	Part Time	Full Time	Full Time	Part Time	Full Time	Full Time
Attend ISSC regularly	No	Yes	Yes	Yes	No	Yes	No	Yes
CCERT participation	No	Yes	Yes	Yes	No	Yes	Yes	Yes
SET participation	No	No	Yes	Yes	No	Yes	Yes	Yes
Have a department computer emergency resp. (DCERT)	No	No	Yes	Yes	No	Yes	Yes	Yes
Systems implemented and configured to security standards	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Employees sign acceptable use agreement	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Passwords changed every 90 days	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Physical security measures in place	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Formal security development lifecycle	No	No	No	Yes	Yes	Yes	Yes	No
Vulnerability assessment scanning performed	No	No	No	Yes	Yes	Yes	No	Yes
Remote access to servers allowed	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	Yes	No	Yes	No	No	No	No	Yes
Have identified specific remote access software	Yes	Yes	No	Yes	No	Yes	Yes	No
Require remote access via VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete computer operating systems	No	No	No	No	No	No	No	Yes
Do you have a technology refresh plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Do you rerquire firewalls on desktops and laptops	No	Yes	Yes	Yes	No	Yes	Yes	No
Host intrusion on servers	No	No	No	No	No	No	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crisis Mgmt Plan	Yes	Yes	No	Yes	No	No	No	Yes
Departmental Security Rating		▨		░				

Color Codes

Good Security Program	░
Some Deficiencies	
Major Weaknesses	▨
Not Applicable	N/A

Information Security Survey 2007

Question	DMH	Mil & Vet	Ombuds	Park Rec	Probat	Pubdef	Pub Hlth	Library
Compliant with Board security policies	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	Yes	N/A	Yes	Yes
Will you be compliant in 2007/2008	N/A	N/A	N/A	N/A	Yes	N/A	Yes	N/A
Designated security officer	Full Time	Part Time	Full Time	Part Time	Full Time	Full Time	Part Time	Full Time
Attend ISSC regularly	Yes	No	Yes	No	Yes	Yes	Yes	Yes
CCERT participation	Yes	No	Yes	No	Yes	Yes	Yes	Yes
SET participation	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Have a department computer emergency resp. (DCERT)	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Systems implemented and configured to security standards	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Employees sign acceptable use agreement	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Passwords changed every 90 days	Yes	No	Yes	Yes	No	Yes	Yes	Yes
Physical security measures in place	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Formal security development lifecycle	No	Yes	Yes	No	No	Yes	No	No
Vulnerability assessment scanning performed	Yes	Yes	No	Yes	No	No	Yes	No
Remote access to servers allowed	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	No	No	No	No	No	No	Yes	No
Have identified specific remote access software	Yes	No	N/A	N/A	Yes	No	Yes	Yes
Require remote access via VPN	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do you have obsolete computer operating systems	No	No	No	No	No	Yes	No	No
Do you have a technology refresh plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you rerquire firewalls on desktops and laptops	No	Yes	Yes	Yes	Yes	No	No	Yes
Host intrusion on servers	No	Yes	Yes	Yes	No	No	No	Yes
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crisis Mgmt Plan	Yes	No	Yes	No	Yes	Yes	No	Yes

Departmental Security Rating								

Color Codes

Good Security Program	░
Some Deficiencies	
Major Weaknesses	▓
Not Applicable	N/A

Information Security Survey 2007

	Safety	DPSS	DPW	Reg Pln	RRCC	Sheriff	TTC
Compliant with Board security policies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
If not,do you have a compliance plan	N/A	N/A	N/A	N/A	N/A	N/A	Yes
Will you be compliant in 2007/2008	N/A	N/A	N/A	N/A	N/A	N/A	Yes
Designated security officer	Part Time	Part Time	Part Time	Part Time	Part Time	Full Time	Full Time
Attend ISSC regularly	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CCERT participation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SET participation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Have a department computer emergency resp. (DCERT)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Systems implemented and configured to security standards	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Employees sign acceptable use agreement	Yes	Yes	Yes	Yes	Yes	No	Yes
Passwords changed every 90 days	Yes	Yes	Yes	Yes	No	Yes	Yes
Physical security measures in place	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Formal security development lifecycle	Yes	Yes	No	Yes	Yes	No	No
Vulnerability assessment scanning performed	Yes	Yes	Yes	No	Yes	No	No
Remote access to servers allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two Factor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	No	No	Yes	No	No	Yes	Yes
Have identified specific remote access software	No	Yes	Yes	No	No	Yes	Yes
Require remote access via VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you have obsolete computer operating systems	No	No	No	No	No	No	Yes
Do you have a technology refresh plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you rerquire firewalls on desktops and laptops	Yes	Yes	No	No	No	Yes	Yes
Host intrusion on servers	Yes	No	No	Yes	No	No	No
Is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software patches current	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crisis Mgmt Plan	Yes	Yes	Yes	Yes	No	No	Yes

Departmental Security Rating	░	□	□	░	□	▓	□

Color Codes

Good Security Program	░
Some Deficiencies	□
Major Weaknesses	▓
Not Applicable	N/A